BACKGROUND INFO

As a member of the cyber security division, your team must handle this incident and the team lead has assigned the issue to you. Below is the timeline of events:

10:30 a.m. – The IT Service Desk receives a report from one of your colleagues at the bank that they have received an email from HR telling all employees to update their timesheets in the company's support portal so the timesheets can be approved on time by their line managers against the next pay day. The colleague clicked the link in the email that opened what looked like the portal. However, following the employee's input of the user credentials, an unfamiliar error page appeared like the one below.

2:00 p.m. – Eight more reports of emails similar to the one reported earlier are received by the IT Service Desk. Upon further investigation, it was found that 62 colleagues across the Risk Department received the same email over the course of two days. The emails directed the users to a fake website to steal their usernames and passwords and download a harmful program.

3:50 p.m. – The IT Service Desk receives calls and emails from more colleagues that the file-shares are not opening and they receive an error when trying to open a Word document they have always been able to open.

TASK

1. What kind of attack has happened and why do you think so?
2. As a cyber security analyst, what are the next steps to take? List all that apply.
3. How would you contain, resolve and recover from this incident? List all answers that apply.
4. What activities should be performed post-incident?

My response

1. The type of attack is a phishing attack. I believe so because the initial emails were sent with the goal of stealing credentials by directing users to a fake website. The later symptoms also suggest that malware could have been installed due to their inability to open a word document that they were always able to open or file shares.

2. The steps to take go as follows:

- **Containment** - Isolate the affected systems to prevent further spread
- **Analyze** - the fishing emails and fake website to understand the attack scope which includes conducting a malware scan on affected systems in order to identify and remove threats.
- **Eradication** - Remove any malware from the systems and ensure that the machines are clean before reconnecting them to the network
- **Recovery** - Restore the affected systems from backups if needed and verify that systems are operational before resuming normal operations
- **Communication** - Notify affected users and especially management about the incident and provide some guidance on password changes, other required actions, and ways to prevent the issue from reoccurring.

3.

Containment:

- Disconnect affected systems from the network
- Change passwords for any accounts that may have been compromised
- Block the phishing email sender along with any malicious domains

Resolution:

- Remove any malicious files or software from the affected systems
- Restore systems and files from trusted backups if needed
- Apply any necessary patches or updates to address vulnerabilities

Recovery:

- Monitor systems for any signs of residual infection/unusual activity
- Confirm that all systems are working properly and securely

4.

Review and Analysis:

- Conduct a thorough investigation of the incident in order to understand how it occurred and the full extent of the impact.
- Analyze logs and other data to identify any gaps in security or response.

Reporting:

- Prepare and submit a detailed incident report to management.
- Document the incident, actions taken, and any lessons learned.

Update Policies and Procedures:

- Review and update incident response procedures based on the findings from the incident.
- Enhance phishing detection and prevention measures.

Training and Awareness:

- Provide training to employees on recognizing and handling phishing attempts.
- Conduct regular security awareness programs to reinforce good practices.

Continuous Improvement:

- Evaluate and improve security controls and practices to prevent future incidents.
- Implement any recommended changes to strengthen the overall security posture.